ABSTRACT

A method and apparatus for performing modular exponentiation is disclosed. An apparatus in accordance with one embodiment of the present invention includes a first modular exponentiator and a second modular exponentiator and a coupling device interposed between the first modular exponentiator and the second modular exponentiator to receive a control signal and to selectively couple the first modular exponentiator to the second modular exponentiator in response to a state of the control signal. In one embodiment, the apparatus has a first mode of operation corresponding to a first state of the control signal wherein the first modular exponentiator is operably separated from the second modular exponentiator and a second mode of operation corresponding to a second state of the control signal wherein the first modular exponentiator is operably coupled to the second modular exponentiator via the coupling device.